基于 Goldwasser-Micali 加密算法的安全子集计算 *

王 倩[a]，任 方[b]，郑 东[b]

(西安邮电大学 a. 计算机学院; b. 通信与信息工程学院, 西安 710121)

摘 要：针对集合间的安全子集问题进行了研究，目前存在解决此类问题的协议大多只能保护一个集合元素的隐私，因此，对于此类问题的研究具有重要的现实意义。在半诚实模型下，利用布隆过滤器及 Goldwasser-Micali 同态加密算法构建了一个安全子集计算协议，并使用安全多方计算中普遍采用的模拟范例证明方法证明了协议的安全性。利用布隆过滤器将拥有大量元素或大数域元素的数据集合映射为较小的数据集合，提升协议的效率及适用范围，同时，借助 Goldwasser-Micali 同态加密算法保证协议的安全性。相关研究大多是基于二次剩余等困难问题，不可抵抗量子攻击，可抵抗量子攻击的安全子集计算是进一步的研究方向。

关键词：安全多方计算；同态加密；布隆过滤器；Goldwasser-Micali 加密算法；安全子集问题

中图分类号：TP309.7 doi: 10.19734/j.issn.1001-3695.2018.09.0758

Secure subset computation based on Goldwasser-Micali encryption algorithm

Wang Qian[a], Ren Fang[b], Zheng Dong[b]

(*a. School of computer science, b. School of Communications & Information Engineering, Xi'an University of Posts & Telecommunications, Xi'an* 710121, *China*)

Abstract: Study the problem of secure subset, most of the existing protocols that solve such problems can only keep the elements of one set private, therefore, it has great practical significance to study this kind of problem. Under the semi-honest model, this paper constructed a secure subset protocol by using Bloom filter and Goldwasser-Micali homomorphic encryption algorithm, and proved the security of the protocol by using common simulation examples in secure multi-party computing. It used the Bloom filter to map a data set with a large number or large number field elements into a smaller data set, improved the efficiency and range of the protocol, at the same time, it used the Goldwasser-Micali homomorphic encryption algorithm to ensure the security of the protocol. Most of the relevant researches are based on the difficult problems such that secondary residuals, it is impossible to resist quantum attacks, and the secure subset computation which can resist quantum attacks is a further research direction.

Key words: secure multi-party computation; homomorphic encryption; bloom filter; Goldwasser-Micali encryption algorithm; secure subset problem

0 引言

网络的迅速发展给多方合作计算中参与者的信息安全带来了巨大的挑战，使安全多方计算[1,2](secure multi-party computation,SMC)成为国际密码学界研究的热点问题。安全多方计算指多个参与者共同秘密计算，且每个参与者的输入信息是保密的，计算结束后，各个参与者除了得到正确的输出结果外，无法获知任何其他输入信息。在借助可信第三方的情况下，安全多方计算非常简单，但在复杂网络中，找到公认的可信第三方是不可能的，因而需要使用其他方式解决该问题。

两个参与者的安全多方计算最早于 1982 年由姚期智教授[1]提出，1987 年，Goldreich 等人[2]提出了可以计算任意函数的基于密码学安全模型的安全多方计算协议，1988 年 Ben 和 Goldwasser[3]提出了多个参与者的安全多方计算，1998 年，Goldreich 对安全多方计算做了比较完整的总结，并提出了安全多方计算的安全性定义。Goldreich 和 Goldwasser 等人的研究推动了安全多方计算的发展，同时激励着研究人员研究各种具有实际应用背景的安全多方计算问题，包括百万富翁问题[1,4,5]、保密的信息比较[6]、保密的统计分析[7]、保密的计算几何[8-10]、保密的数据挖掘[11]、保密的集合问题[12~14]等。

Goldwasser-Micali 加密算法是 1982 年由 Goldwasser[15]等人提出的，其安全性基于二次剩余困难问题，该加密算法具有异或同态性。文献[16,17]基于 Goldwasser-Micali 加密算法提出了隐私交集基数协议，其中文献[16]以布隆过滤器(Bloom filter)[18]为工具。本文利用 Goldwasser-Micali 同态加密算法和布隆过滤器，在半诚实模型下，构建了一个安全子集计算协议，并对其进行了正确性、安全性证明。

1 预备知识

1.1 安全子集问题

假设 Alice 输入集合 $A=\{a_1,a_2,\ldots,a_m\}$，Bob 输入集合 $B=\{b_1,b_2,\ldots,b_n\}$，Alice 和 Bob 想要在不向对方泄露其集合元素任何信息的情况下，输出集合 B 是否是集合 A 的子集，即判断 $B\subseteq A$？的问题称为安全子集问题[12]。

收稿日期：2018-09-28；**修回日期：**2018-11-20 **基金项目：**国家自然科学基金资助项目（61472472）；陕西省自然科学基金资助项目（2015JQ6262）

作者简介：王倩（1990-），女（通信作者），新疆伊宁人，助理工程师，硕士，主要研究方向为信息安全（wangqian@xupt.edu.cn）；任方（1981-），男，陕西西安人，副教授，博士，主要研究方向为密码学、信息安全；郑东（1964-），男，山西翼城人，教授，博导，博士，主要研究方向为密码学、云存储安全.

1.2　二次剩余问题

对于整数 $n>1$，定义 $Z_n^*=\{a\in Z_n:\gcd(a,n)=1\}$。当存在 $d\in Z_n$，使得 $d^2\equiv a \bmod n$，称 a 为模 n 的二次剩余；否则称 a 为模 n 的二次非剩余。判断 a 是否为模 n 的二次剩余的问题称为模 n 的二次剩余问题[17]。

1.3　Goldwasser-Micali 同态加密方案

Goldwasser-Micali(GM)加密方案是第一个证明为 CPA 安全的公钥加密方案，其安全性依赖于从合数模的二次非剩余中区分二次剩余困难性假设[19]。具体如下。

a）密钥生成算法。用户随机生成两个大素数 p 和 q，计算 $n=pq$，z 是模 n 的二次非剩余中的随机数。系统公钥 $pk=(n,z)$，系统私钥 $sk=(p,q)$。

b）加密算法。明文空间是 $\{0,1\}$，对于明文 $x\in\{0,1\}$，加密方选取秘密随机数 $r\in Z_n^*$，利用系统公钥 pk 计算密文 $E(x)=r^2z^x \bmod n$。

c）解密算法。对于密文 $E(x)$，判断 $E(x)$ 是否为模 n 的二次剩余，若 $E(x)$ 是模 n 的二次剩余，则明文 $D(E(x))=0$；若 $E(x)$ 不是模 n 的二次剩余，则 $D(E(x))=1$。

GM 加密系统的安全性是基于模 n 的二次剩余问题。对于私钥的拥有者，知道大整数 n 的因子分解，求解模 n 的二次剩余问题是容易的；而对于攻击者，无法获知 n 的因子分解，求解模 n 的二次剩余问题是困难的，继而保证了该加密方案的安全性。

该加密方案具有如下性质：

a）异或同态性。设明文 x_1 和 x_2 的密文为 $E(x_1)$ 和 $E(x_2)$，则 $E(x_1)\cdot E(x_2)$ 是 $x_1\oplus x_2$ 的密文，即 $D(E(x_1)\cdot E(x_2))=x_1\oplus x_2$；

b）非运算同态性。即 $E(x)\cdot z=E(x\oplus 1)=E(\bar{x})$；

c）重复加密随机性。即 $D(E(x)\cdot E(0))=D(E(x))$。

1.4　布隆过滤器（Bloom Filter）

布隆过滤器（Bloom filter）是 1970 年由 Bloom[18]提出的一种基于多个哈希函数映射压缩参数空间的数据结构，由一个很长的二进制向量和一组 hash 函数构成，通过 hash 函数将拥有大量元素或大数域元素的数据集合映射为较小的数据集合，如需判断一个元素是否在集合中，将元素用相同的 hash 函数处理，并将产生的 hash 值与布隆过滤器中的数据集合比较，相等说明元素在集合中，否则，元素不在集合中。具体工作过程如下：

a）初始化。设集合 B 的布隆过滤器为 $BF_B=(\omega,n,k,H)$，ω 是 BF_B 的向量组大小，$H=(h_1,h_2,\ldots,h_k)$ 是 k 个相互独立的 hash 函数，在初始状态下，将 BF_B 的每一位都置为 0。

b）存储映射过程。集合 B 中的任意元素 b 经过布隆过滤器的 hash 映射时，每个映射值所对应的 BF_B 中的位置均被置为 1，即 $BF_B[h_j(b)]=1$，$j=1,2,\ldots,k$，所有 B 中的元素都映射存储在 BF_B 中后，BF_B 代表集合 B。如图 1 所示。

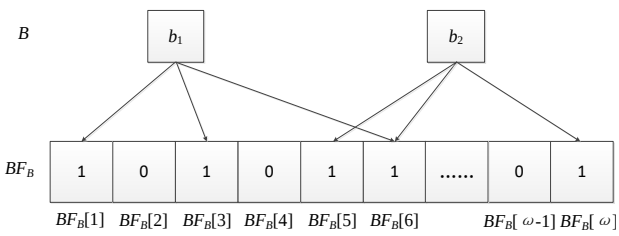

图 1　布隆过滤器的存储映射过程

Fig. 1　Stored mapping procedure for bloom filter

c）查找映射过程。若要判断元素 b' 是否是集合 B 中的元素，需要对元素 b' 进行 hash 映射，计算并验证当 $j=1,2,\ldots,k$ 时，$BF_B[h_j(b')]$ 是否均为 1，若其中有一位为 0，则 b' 不是集合 B 中的元素，否则 b' 有较高的几率是集合 B 中的元素。如图 2 所示。

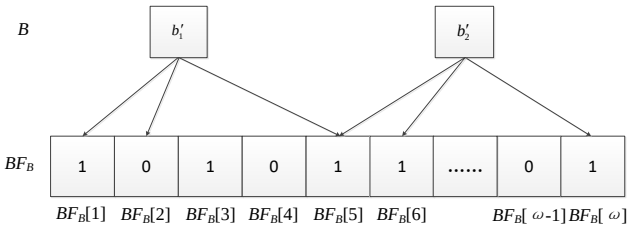

图 2　布隆过滤器的查找映射过程

Fig. 2　Find mapping procedure for bloom filter

布隆过滤器的优点是空间及查询效率远高于其他算法，不需要存储元素本身，仅需要几个简单的字节位即可保存一个元素；缺点是会对一些未处理或不属于集合的元素产生误判，随着存入查询频率的增多，误判率越大，例如：如果 b 是集合 B 中的元素，$j=1,2,\ldots,k$ 时 $BF_B[h_j(b')]$ 一定为 1；如果 b 不是集合 B 中的元素，$j=1,2,\ldots,k$ 时 $BF_B[h_j(b')]$ 可能为 1。

1.5　半诚实模型下的安全性

假设有一个可信第三方（trusted third party,TTP），在任何情况下都不会泄露任何不该泄露的信息。多个参与者联合进行安全计算时，将秘密信息发送给可信第三方，由可信第三方完成运算并将结果发送给各个参与者，这种计算模型称为可信第三方模型。计算结束后，参与者只得到可信第三方发送给自己的计算结果而得不到任何其他信息，这种可信第三方模型具有最高的安全性，但是现实生活中很难找到可以完全信任的第三方机构，因此，这种可信第三方模型也称为理想模型。

在目前的安全多方计算研究中，很少使用理想模型。在半诚实模型下，实际的安全多方计算协议可通过与理想的安全多方计算协议对比来检验其安全性，目前普遍采用的安全性证明方法模拟范例就是基于此类方式证明，如果实际的安全多方计算协议不比理想的安全多方计算协议泄露更多信息，则证明这个协议是安全的[20]。本文采用的安全性证明方式即为模拟范例。

假设参与者 P_1 和 P_2 要计算函数 f：

$$\{0,1\}^*\times\{0,1\}^*\mapsto\{0,1\}^*\times\{0,1\}^*$$

其中：$f(x,y)=(f_1(x,y),f_2(x,y))$，$\Pi$ 是参与者 P_1 和 P_2 计算函数 f 的一个双方协议。

参与者 P_1 和 P_2 在协议 Π 的执行过程中得到的信息分别记为

$$\text{view}_1^{\Pi}(x,y)=(x,r^1,m_1^1,m_2^1,\ldots,m_t^1)$$

$$\text{view}_2^{\Pi}(x,y)=(y,r^2,m_1^2,m_2^2,\ldots,m_t^2)$$

其中：r^i 表示参与者 P_i 产生的随机数，m_j^i 表示 P_i 收到的第 j 条信息。协议执行完后，参与者 P_i 的输出结果记为 $\text{output}_i^{\Pi}(x,y)$。

对于函数 $f=(f_1,f_2)$，本文称协议 Π 在半诚实模型下安全的计算函数 f，当且仅当存在概率多项式时间算法 S_1 和 S_2，满足

$$\{S_1(x,f_1(x,y)),f_2(x,y)\}\overset{c}{\equiv}\{\text{view}_1^{\Pi}(x,y),\text{output}_2^{\Pi}(x,y)\}$$

$$\{f_1(x,y),S_2(y,f_2(x,y))\}\overset{c}{\equiv}\{\text{output}_1^{\Pi}(x,y),\text{view}_2^{\Pi}(x,y)\}$$

其中：$\overset{c}{\equiv}$ 表示随机变量簇的计算不可区分[17]。

2　基于 Goldwasser-Micali 加密算法的安全多方子集计算

本节基于Goldwasser-Micali同态加密算法的重复加密随机性，利用布隆过滤器，在半诚实模型下构建了一个安全子集计算协议，并给出了正确性证明，同时，利用模拟范例证明方式对协议进行了安全性证明。协议通过使用布隆过滤器，可将拥有大量元素或大数域元素的数据集合，通过 hash 函数映射为较小的数据集合，提升了协议的效率及适用范围。具体协议如协议 1。

2.1　协议 1

输入：Alice 输入集合 $A=\{a_1,a_2,\ldots,a_m\}$，Bob 输入集合 $B=\{b_1,b_2,\ldots,b_n\}$。

输出：集合 B 是否是集合 A 的子集，即 $B\subseteq A$？。

a）Alice 和 Bob 共同协商参数 $\omega,k,H=(h_1,h_2,\ldots,h_k)$，并分别构建其输入集合的 Bloom filter，其中集合 A 的 Bloom filter 记为 BF_A，集合 B 的 Bloom filter 记为 BF_B；

$$BF_A=(BF_A[1],BF_A[2],\ldots,BF_A[\omega])$$
$$BF_B=(BF_B[1],BF_B[2],\ldots,BF_B[\omega])$$

b）Alice 生成 Goldwasser-Micali 加密系统的公私钥对 (pk,sk)，公开其公钥 $pk=(n,z)$，并用公钥 pk 逐比特加密得 $E(BF_A)$，将加密后的 $E(BF_A)$ 发送给 Bob；

$$E(BF_A)=(E(BF_A[1]),E(BF_A[2]),\ldots,E(BF_A[\omega]))$$

c）Bob 根据 BF_B 中为 1 的位 $\{BF_B[i_1],BF_B[i_2]\ldots,BF_B[i_t]\}$，从 $E(BF_A)$ 选取 $\{E(BF_A[i_1]),E(BF_A[i_2]),\ldots,E(BF_A[i_t])\}$。描述成伪代码如下：

```
for  i=1  to  ω
    if  BF_B[i]=1
        return  E(BF_A[i])
end
```

d）Bob 随机生成 t 个数 $\{r_1,r_2,\ldots,r_t\}$，并用 $\{r_1,r_2,\ldots,r_t\}$ 对 $\{E(BF_A[i_1]),E(BF_A[i_2]),\ldots,E(BF_A[i_t])\}$ 进行加密得：

$$\{C_1,C_2,\ldots,C_t\}$$
$$=\{E(BF_A[i_1])\cdot r_1^2 \bmod n,E(BF_A[i_2])\cdot r_2^2 \bmod n,\ldots,E(BF_A[i_t])\cdot r_t^2 \bmod n\}$$

并将 $\{C_1,C_2,\ldots,C_t\}$ 发送给 Alice，其中 n 是密钥参数中的模数；

e）Alice 对 $\{C_1,C_2,\ldots,C_t\}$ 进行解密得 $\{d_1,d_2,\ldots,d_t\}$：

$$\{d_1,d_2,\ldots,d_t\}=\{D(C_1),D(C_2),\ldots,D(C_t)\},$$

输出 $\{d_1,d_2,\ldots,d_t\}$，如果 $\{d_1,d_2,\ldots,d_t\}$ 均为 1，那么 $B\subseteq A$，否则 $B\not\subset A$。

其中Bob执行协议部分，即协议1的第c)d)步骤如图3所示，假设集合 B 的布隆过滤器 BF_B 中的某些位为 1。

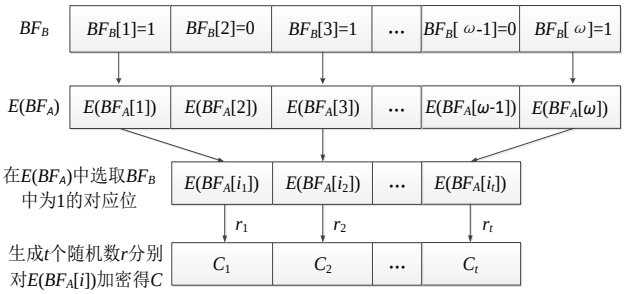

图 3　Bob 执行协议部分框图

Fig. 3　Bob executes part of the protocol block diagram

2.2　正确性分析

在半诚实模型下，Alice 和 Bob 都严格遵循协议 1。

对于任意 $i=1,2,\ldots,t$，均有

$$r_i^2 \bmod n=r_i^2\cdot z^0 \bmod n=E(0),$$

即 $r_i^2 \bmod n$ 可视为“0”的密文，根据 Goldwasser-Micali 同态加密方案的重复加密随机性可知：

$$E(BF_A[i_1])\cdot r_1^2 \bmod n=E(BF_A[i_1])\cdot E(0)=E(BF_A[i_1])$$
$$\vdots$$
$$E(BF_A[i_t])\cdot r_t^2 \bmod n=E(BF_A[i_t])\cdot E(0)=E(BF_A[i_t])$$

相当于对 $\{E(BF_A[i_1]),E(BF_A[i_2]),\ldots,E(BF_A[i_t])\}$ 进行了重复加密，因此

$$\{d_1,\ldots d_t\}$$
$$=\{D(C_1),\ldots,D(C_t)\}$$
$$=\{D(E(BF_A[i_1])\cdot r_1^2 \bmod n),\ldots,D(E(BF_A[i_t])\cdot r_t^2 \bmod n)\}$$
$$=\{D(E(BF_A[i_1])),\ldots,D(E(BF_A[i_t]))\}$$
$$=\{BF_A[i_1],\ldots,BF_A[i_t]\}$$

若 $\{BF_A[i_1],BF_A[i_2],\ldots,BF_A[i_t]\}$ 均为 1，说明对于任意元素 $x\in B$，都有 $x\in A$，即 $B\subseteq A$；

若 $\{BF_A[i_1],BF_A[i_2],\ldots,BF_A[i_t]\}$ 中至少有一位为 0，说明存在元素 $x\in B$，使得 $x\notin A$，即 $B\not\subset A$。

由此可知，协议 1 正确。

3　安全性分析

在半诚实模型下，Alice 和 Bob 都严格遵循协议 1，允许他们借助自己在执行协议过程中的全部中间信息，去推测对方的秘密输入信息。

令 $f_1(x,y)=\{d_1,d_2,\ldots,d_t\}$，$f_2(x,y)=\perp$（空字符），下面构造概率多项式时间模拟器 S_1 和 S_2，使下面两个关系成立。

$$\{S_1(x,f_1(x,y)),f_2(x,y)\}\overset{c}{\equiv}\{\text{view}_1^{\Pi}(x,y),\text{output}_2^{\Pi}(x,y)\}\tag{3-1}$$

$$\{f_1(x,y),S_2(y,f_2(x,y))\}\overset{c}{\equiv}\{\text{output}_1^{\Pi}(x,y),\text{view}_2^{\Pi}(x,y)\}\tag{3-2}$$

1）构造模拟器 S_1，使得等式（3-1）成立

执行完协议 1 后，Alice 的 view 为

$$view_1^{\Pi}(x,y)=(A,R_1,\{C_1,C_2,\ldots,C_t\}),$$

其中 R_1 是 Alice 生成的随机数，$\{C_1,C_2,\ldots,C_t\}$ 是 Alice 从 Bob 处收到的信息。

S_1 的模拟过程如下：

S_1 根据集合 A 和参数 ω,k,H 构建集合 A 的 Bloom filter 记为 BF_A；

由于 S_1 拥有 $\{d_1,d_2,\ldots,d_t\}$，它根据 $\{d_1,d_2,\ldots,d_t\}$ 构造集合 B 的 Bloom filter 记为 BF_B'，使得 BF_B' 中为 1 的位

$$\{BF_B'[i_1],BF_B'[i_2],\ldots,BF_B'[i_t]\},$$

对应的 BF_A 中分别为

$$BF_A[i_1]=d_1,BF_A[i_2]=d_2,\ldots,BF_A[i_t]=d_t;$$

S_1 用公钥 pk 对 $\{BF_A[i_1],BF_A[i_2],\ldots,BF_A[i_t]\}$ 加密得

$$\{E'(BF_A[i_1]),E'(BF_A[i_2]),\ldots,E'(BF_A[i_t])\};$$

S_1 随机生成 t 个数 $\{r_1',r_2',\ldots,r_t'\}$，并对

$$\{E'(BF_A[i_1]),E'(BF_A[i_2]),\ldots,E'(BF_A[i_t])\}$$

进行加密，得：

$$\{C_1',\ldots,C_t'\}$$
$$=\{E'(BF_A[i_1])\cdot r_1'^2 \bmod n,\ldots,E'(BF_A[i_t])\cdot r_n'^2 \bmod n\}$$

$S_1(x,f_1(x,y))=(A,R_1',\{C_1',C_2',\ldots,C_t'\})$，其中 R_1' 是 S1 生成的随机数。

下面证明 $\{S_1(x,f_1(x,y)),f_2(x,y)\}\overset{c}{\equiv}\{\text{view}_1^{\Pi}(x,y),\text{output}_2^{\Pi}(x,y)\}$ 成

立，其中 $f_2(x,y)=\text{output}_2^{\Pi}(x,y)=\perp$。只需证明

$$S_1(x,f_1(x,y))\overset{c}{\equiv}\text{view}_1^{\Pi}(x,y),$$

即证明下面的关系成立：

$$\left(A,R_1',\{C_1',C_2',\ldots,C_t'\}\right)\overset{c}{\equiv}(A,R_1,\{C_1,C_2,\ldots,C_t\})。$$

由于 R_1' 和 R_1 分别是 S_1 和 Alice 生成的随机数，因此 $\{R_1'\}\overset{c}{\equiv}\{R_1\}$，又 $C_i=E(BF_A[i])\cdot r_i^2 \bmod n$，$C_i'=E'(BF_A[i])\cdot r_i'^2 \bmod n$，其中 r_i 与 r_i' 分别是 Bob 和 S_1 选取的随机数，故 C_i 和 C_i' 是随机的，$\{C_i\}\overset{c}{\equiv}\{C_i'\}$，

综上可得：

$$\{S_1(x,f_1(x,y)),f_2(x,y)\}\overset{c}{\equiv}\{\text{view}_1^{\Pi}(x,y),\text{output}_2^{\Pi}(x,y)\}。$$

2）构造模拟器 S_2，使得等式（3-2）成立

执行完协议 1 后，Bob 的 view 为

$$view_2^{\Pi}(x,y)=(B,R_2,\{E(BF_A[1]),E(BF_A[2]),\ldots,E(BF_A[\omega])\}),$$

其中：R_2 是 Bob 生成的随机数，$\{E(BF_A[1]),E(BF_A[2]),\ldots,E(BF_A[\omega])\}$ 是 Bob 从 Alice 处收到的信息。

S_2 的模拟过程如下：

S_2 根据集合 B 和参数 ω,k,H 构建集合 B 的 Bloom filter 记为 BF_B；

由于 S_2 拥有 $\{d_1,d_2,\ldots,d_t\}$，它构造集合 A 的 Bloom filter 记为 $BF_A'=\{BF_A'[1],BF_A'[2],\ldots,BF_A'[\omega]\}$，使得 BF_B 中为 1 的位

$$\{BF_B[i_1],BF_B[i_2],\ldots,BF_B[i_t]\},$$

对应的 BF_A' 中分别为

$$BF_A'[i_1]=d_1,BF_A'[i_2]=d_2,\ldots,BF_A'[i_t]=d_t;$$

S_2 用公钥 pk 对 BF_A' 加密得

$$\{E'(BF_A'[1]),E'(BF_A'[2]),\ldots,E'(BF_A'[\omega])\};$$

S_2 随机生成 t 个数 $\{r_1',r_2',\ldots,r_t'\}$，并对

$$\{E'(BF_A'[1]),E'(BF_A'[2]),\ldots,E'(BF_A'[\omega])\}$$

进行加密，得

$$\{C_1',\ldots,C_t'\}=\{E'(BF_A[i_1])\cdot r_1'^2 \bmod n,\ldots,E'(BF_A[i_t])\cdot r_n'^2 \bmod n\}$$

$$S_2(f_2(x,y),y)=\left(B,R_2',\{E'(BF_A'[1]),E'(BF_A'[2]),\ldots,E'(BF_A'[\omega])\}\right),$$

其中 R_2' 是 S2 生成的随机数。

下面证明 $\{f_1(x,y),S_2(y,f_2(x,y))\}\overset{c}{\equiv}\{\text{output}_1^{\Pi}(x,y),\text{view}_2^{\Pi}(x,y)\}$ 成立，其中 $f_1(x,y)=\text{output}_1^{\Pi}(x,y)=\{d_1,d_2,\ldots,d_t\}$，只需证明

$$S_2(y,f_2(x,y))\overset{c}{\equiv}\text{view}_2^{\Pi}(x,y),$$

即证明下面的关系成立：

$$\left(B,R_2',\{E'(BF_A'[1]),\ldots,E'(BF_A'[\omega])\}\right)\overset{c}{\equiv}(B,R_2,\{E(BF_A[1]),\ldots,E(BF_A[\omega])\})$$

由于 R_2' 和 R_2 分别是 S_2 和 Bob 生成的随机数，因此 $\{R_2'\}\overset{c}{\equiv}\{R_2\}$，又根据 Golewasser-Micali 加密算法，$E(BF_A[i])$ 和 $E'(BF_A'[i])$ 具有随机性，$\{E(BF_A[i])\}\overset{c}{\equiv}\{E'(BF_A'[i])\}$，

综上可得：

$$\{f_1(x,y),S_2(y,f_2(x,y))\}\overset{c}{\equiv}\{\text{output}_1^{\Pi}(x,y),\text{view}_2^{\Pi}(x,y)\}。$$

定理证毕。

综上，本文基于 Goldwasser-Micali 同态加密算法构建的安全子集协议在半诚实模型下是安全的，同时，通过使用布隆过滤器，使协议具有较高的效率，并且扩大了协议的适用范围。

4　结束语

保密的判断集合间的关系对于现实生活中的实际意义越来越重要，现有的协议大多只能保护一个集合中元素的隐私。为此，本文基于 Goldwasser-Micali 同态加密算法在半诚实模型下构建了一个的安全子集计算协议，并对协议进行了正确性及安全性证明。协议通过使用布隆过滤器，可判断拥有大量元素或大数域元素的集合间关系，将其映射为较小的数据集合，提升了协议的效率及适用范围。目前的相关研究大多是基于二次剩余等困难问题，不可抵抗量子攻击，随着量子计算机的迅速发展，研究可以抵抗量子攻击的安全子集计算具有重要的意义，将是进一步的研究方向。

参考文献：

[1] Yao A C. Protocols for secure computations [C]//Proc of Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 1982: 160-164.

[2] Goldreich O, Micali S, Wigderson A. How to play any mental game [C]//Proc of the 19th ACM Symposium on Theory of Computing.New York: ACM Press, 1987: 218-229.

[3] Ben-Or M, Goldwasser S, Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation [C]// Proc of ACM Symposium on Theory of Computing.New York:ACM Press, 1988: 1-10.

[4] Li Shundong, Guo Yimin, Zhou Sufang, *et al.* Efficient protocols for the general millionaires'problem [J]. Chinese Journal of Electronics, 2017, 26 (4): 696-702.

[5] Grigoriev D, Kish L B, Shpilrain V. Yao's millionaires'problem and public-key encryption without computational assumptions [J]. Interna tional Journal of Foundations of Computer Science, 2017, 28 (4): 11.

[6] 秦静，张振峰，冯登国，等. 无信息泄漏的比较协议 [J]. 软件学报，2004, 15 (3): 421-427. (Qin Jing, Zhang Zhenfeng, Feng Dengguo, *et al.* A protocol of comparing information without leaking [J]. Journal of Software, 2004, 15 (3): 421-427.)

[7] 杨波，禹勇，杨中皇. 恶意敌手模型下的安全点乘协议 [J]. 计算机科学与技术，2013, 28 (1): 152-158. (Yang Bo, Yu Yong, Yang Zhong huang. A secure scalar product protocol against malicious adversaries [J]. Journal of Computer Science and Technology, 2013, 28 (1): 152-158.)

[8] Li Shundong, Wu Chunying, Wang Daoshun, *et al.* Secure multiparty computation of solid geometric problems and their applications [J]. Information Sciences, 2014, 282: 401-413.

[9] He Feng, Wang Ting. Research and application of secure multi-party computation in several computational geometry problems [C]// Proc of International Conference on Industrial Control and Electronics Engineering. Piscataway, NJ: IEEE Press, 2012: 1434-1437.

[10] 辛欣，郝林，汤瑜. 空间两平行直线间距离的保密计算协议 [J]. 计算机应用研究, 2013, 30 (5): 1530-1532. (Xin Xin, Hao Lin, Tang Yu. Privacy-preserving computational protocol on minimum distance between two three-dimension parallel straight line [J]. Application Research of Computers, 2013, 30 (5): 1530-1526.)

[11] Pathak F A N, Pandey S B S. An efficient method for privacy preserving data mining in secure multiparty computation [C]//Proc of Nirma University International Conference on Engineering. Piscataway, NJ: IEEE Press, 2013.

[12] Zhou Sufang, Li Shundong, Dou Jiawei, *et al.* Efficient secure multiparty subset computation [J]. Security & Communication Networks, 2017, 2017 (3): 1-11.

[13] 李顺东，周素芳，郭奕旻，等. 云环境下集合隐私计算 [J]. 软件学报, 2016, 27 (6): 1549-1565. (Li Shundong, Zhou Sufang, Guo Yimin, *et al.* Secure set computing in cloud environment [J]. Journal of Software, 2016, 27 (6): 1549-1565.)

[14] Bogdanov D, Niitsoo M, Toft T, *et al.* High-performance secure multi-party computation for data mining applications [J]. International Journal of Information Security, 2012, 11 (6): 403-418.

[15] Goldwasser S, Micali S. Probabilistic encryption & how to play mental poker keeping secret all partial information [C]//Proc of the 14th ACM Symposium on Theory of Computing.New York: ACM Press, 1982: 365-377.

[16] Debnath S K, Dutta R. Secure and efficient private set intersection cardinality using Bloom filter [C]//Proc of International Information Security Conference. Springer International Publishing, 2015: 209-226.

[17] 马敏耀，陈松良，左羽. 基于 Goldwasser-Micali 加密系统的隐私交集基数协议研究 [J].计算机应用研究, 2018, 35(9): 2748-2751. (Ma Minyao, Chen Song liang, Zuo Yu. Research on private set intersection cardinality protocol based on Goldwasser-Micali encryption system [J].Application Research of Computers, 2018, 35(9): 2748-2751..)

[18] Heydon A, Najork M. Mercator: a scalable, extensible web crawler [J]. World Wide Web-internet & Web Information Systems, 1999, 2 (4): 219-229.

[19] 孙茂华. 安全多方计算及其应用研究 [D]. 北京：北京邮电大学, 2013. (Sun Maohua. Research on secure multi-party comptation and its application [D]. Beijing: Beijing University of Posts and Telecommunications, 2013.)

[20] 周素芳，窦家维，郭奕旻，等. 安全多方向量计算 [J]. 计算机学报, 2017, 40 (5): 1134-1150. (Zhou Sufang, Dou Jiawei, Guo Yimin, *et al.* Secure multiparty vector computation [J]. Chinese Journal of Computers, 2017, 40 (5): 1134-1150.)